

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A) 平2-151892

⑬ Int. Cl.⁵

識別記号

庁内整理番号

⑭ 公開 平成2年(1990)6月11日

G 09 C 1/00
G 06 F 7/72

7368-5B
7056-5B

審査請求 未請求 請求項の数 1 (全 11 頁)

⑮ 発明の名称 べき乗剰余演算装置

⑯ 特 願 昭63-307361

⑰ 出 願 昭63(1988)12月5日

⑱ 発 明 者 松 崎 な つ め 大阪府門真市大字門真1006番地 松下電器産業株式会社内
⑲ 発 明 者 館 林 誠 大阪府門真市大字門真1006番地 松下電器産業株式会社内
⑳ 出 願 人 松下電器産業株式会社 大阪府門真市大字門真1006番地
㉑ 代 理 人 弁理士 栗 野 重 孝 外 1 名

明 細 書

1. 発明の名称

べき乗剰余演算装置

2. 特許請求の範囲

素数 p と素数 q の積 n を法とし、正整数 d をべき数として入力 x のべき乗剰余演算を行う装置であり、前記正整数 d と素数 q の値を保持し、かつその値が外部から決定あるいは推測できないように構成された第1の計算装置と、この第1の計算装置から送出された第1のデータに対して所定の計算を行いその結果を第2のデータとして前記第1の計算装置に送出する第2の計算装置からなり、前記第1の計算装置は前記素数 p と q の積 n と、前記正整数 d を $p-1$ で除した剰余 d_1 と、前記正整数 d を $q-1$ で除した剰余 d_2 を計算してこれらの結果を前記第1のデータとして前記第2の計算装置に送出し、さらに前記第2の計算装置から送出された前記第2のデータを前記素数 p と q を用いて結合し、法を前記の数 n とし、前記正整数 d をべき数とする入力 x のべき乗剰余値を求め

るものであり、前記第2の計算装置は前記第1の計算装置から送出された前記第1のデータから、前記整数 n を法とし前記 d_1 をべき数とする前記正整数 x のべき乗剰余数 y_1 と、前記整数 n を法とし前記 d_2 をべき数とする前記正整数 x のべき乗剰余数 y_2 を計算し、この結果を前記第2のデータとして前記第1の計算装置に対して送出することを特徴とするべき乗剰余演算装置。

3. 発明の詳細な説明

産業上の利用分野

本発明はICカードなど計算能力のあまり高くないデバイスが補助装置を用いてRSA暗号などの公開鍵暗号の基本演算であるべき乗剰余演算を行うべき乗剰余演算装置に関するものである。

従来の技術

RSA暗号を代表とする公開鍵暗号方式は

- ① 鍵配送が容易である。
- ② 秘密に保持する鍵の種類が少ない。
- ③ 安全な認証機能(デジタル署名機能)がある。

などの長所を持つ反面、その安全性を保证するためには例えば612ビット程度の長語長の数のべき乗剰余演算、すなわち $y = x^d \bmod n$ (x, d, n : 612ビット)を行う必要がある。なお、ここで'^'はべき乗演算を示し、 $\bmod n$ は n で除したときの剰余を示す。以降これらの記述を用いる。

この長語長の演算を例えば8ビットや16ビットの汎用CPUのソフトウェアで実現すると、数10秒といった非常に長い演算時間を要す。

一方、ICカードは計算・記憶・情報保護能力を備え、携帯に便利なデバイスであり、特に金融関係に有望である。ICカードを金融関係に用いる場合、送られてきた暗号文の送信者が偽者でないことを確認できる認証機能が特に重要になってくる。前記したように公開鍵暗号方式は安全な認証機能を有し、この点でICカードにおいて公開鍵暗号方式を実現する義務がある。ところがICカードの計算能力、記憶能力はあまり高くなく、前述したように膨大な演算量を必要とする公開鍵

暗号方式をICカード単独で実現することは実用上不可能である。そこでこの基本演算であるべき乗剰余演算を計算能力、記憶能力のすぐれている補助装置(たとえばPOS端末など)の助けをかりて行うことを考える。ただし、この補助装置は必ずしもICカードにとって信頼できるものではないため、ICカード内の秘密の情報は漏らさないことが必要である。この方法を「補助装置を用いたべき乗剰余演算装置」と称する。

従来の補助装置を用いたべき乗剰余演算装置としてはたとえば文献「加藤、松本・安全な計算依頼法について」1988年暗号と情報セキュリティシンポジウム」に示されている。

第2図に従来のべき乗剰余演算装置における第1の例の構成図を示す。100はICカード、101は補助装置である。102、103はそれぞれICカードにおける秘密のデータ p, q を格納している p 格納部と q 格納部、104は p と q の積を計算して n を生成する n 生成部、105は n を公開する n 公開部である。106はICカー

ドにおける秘密のデータ d を格納している d 格納部、107は d を次の(1)式のように表現し、これを満たす $D = \{d_1, \dots, d_m\}$, $F = \{f_1, \dots, f_m\}$ を求める d 分割部である。

$$d = d_1 \times f_1 + \dots + d_m \times f_m \bmod \lambda(n) \quad \dots\dots(1)$$

ただし、 $\lambda(n)$ は $p-1$ と $q-1$ の最小公倍数とする。

また、 $d_i < (p-1) \times (q-1)$, $f_i = 1$ または 0 ($i=1 \sim m$) である。

108は前記 D を補助装置101に送信する D 送信部、109は前記 F を格納する F 格納部である。110はデータ x を格納している x 格納部、111は x を補助装置に送信する x 送信部である。112は補助装置内で公開数 n を受信する n 受信部、113、114はそれぞれICカードからの D 、 x を受信する D 受信部、 x 受信部である。116は112~114のデータを用いて次の(2)式を計算して $Y' = (y_1, \dots, y_m)$ を求めるべき乗剰余計算部である。

$$y_i = x^{d_i} \bmod n \quad (i=1 \sim m) \quad \dots\dots(2)$$

116は前記 Y' をICカードに送信する Y' 送信部である。117はICカード内で Y' を受信する Y' 受信部、118は前記 Y' , n, F を用いて(3)式の計算を行い y を生成する y 生成部である。

$$y = (y_1^{f_1}) \times \dots \times (y_m^{f_m}) \bmod n \quad \dots\dots(3)$$

119は前記 y を格納する y 格納部である。

なお、前記102~111、117~119はICカードを100に含まれ、112~116は補助装置に含まれる。また、102~109、112~113は初期化のときのみ動作する。

次に、以上説明した従来のべき乗剰余演算装置の動作を、RSA暗号の復号化を行う場合を例に説明する。

<RSA暗号の復号化>

x を612ビットの暗号文、 d を秘密の復号化鍵(612ビット)、 n を612ビットの公開値とすると、以下の(4)式の演算を行うことによ

7

て512ビットの復号文 y を得る。

$$y = x^d \bmod n \quad (x, d, n: 512 \text{ ビット}) \quad \dots\dots\dots(4)$$

ただし、 $n = p \times q$ ($p, q: 256$ ビットの素数)であり、このRSA暗号の復号化を行う主体であるICカードだけは n の素因数分解 p, q を知っているとする。

<初期化>

- ① ICカード内の p, q (ICカードの秘密の情報)がそれぞれ p 格納部102, q 格納部103に格納されている。 n 生成部104において p と q の積を計算して n 公開部105に格納する。 n はこの n 公開部105により広く公開される。
- ② ICカード内の d (ICカードの秘密の情報)が d 格納部106に格納されている。 d 分割部107において d を前記(1)式のように表現し、これを満たす $D = \{d_1, \dots, d_m\}$, $F = \{f_1, \dots, f_m\}$ を求める。ただしここで $d_i < (p-1) \times (q-1)$, $f_i = 1$ ま

9

部115の出力をICカード内の Y' 受信部117に送信する。

- ⑤ ICカード内の y 生成部118は補助装置が求めた Y' と F 格納部に格納されている F を用いて前記(3)式を計算する。

(3)式は補助装置が計算した $Y' = \{y_1, \dots, y_m\}$ のうち対応する $F = \{f_1, \dots, f_m\}$ が"1"であるものを法 n で乗算して y を得ることを意味している。

なお、上記の方法で求めた y は(4)式を満たしている n 未満の正整数である。それは次の(5)より明らかである。

前記(3)式

$$\begin{aligned} &= (y_1^{f_1}) \times \dots \times (y_m^{f_m}) \\ &\quad \bmod n \\ &= (x^{d_1} \bmod n)^{f_1} \times \dots \times (x^{d_m})^{f_m} \bmod n \\ &= x^{(d_1 \times f_1 + \dots + d_m \times f_m)} \\ &\quad \bmod l(n) \bmod n \\ &= x^d \bmod n \quad \dots\dots\dots(5) \end{aligned}$$

たは0である。

D は D 送信部108より補助装置に送信される。 F はICカード内の F 格納部109に格納される。

- ③ 補助装置内の n 受信部112は公開されている n を受信する。
- ④ 補助装置内の D 受信部113はICカードより送信された D を受信する。

<繰り返し処理>

以下の処理は512ビットを1ブロックとする暗号文の数だけ繰り返す。

- ① 暗号文1ブロックをICカード内の x 格納部に格納する。
- ② ICカード内の x 送信部111より補助装置内の x 受信部114に暗号文 x を送信する。
- ③ 補助装置のべき乗剰余計算部116は暗号文 x , 公開値 n , ICカードから受け取った D を用いて前記(2)式の演算を行い、 $Y' = \{y_1, \dots, y_m\}$ を得る。
- ④ 補助装置内の Y' 送信部は前記べき乗剰余計算

10ページ

また、補助装置が総当たりによってICカードの持つ秘密の鍵 d の探索を行う場合、その鍵の候補数は、 $F = \{f_1, \dots, f_m\}$ のうち $f_i = 1$ となる i の個数を L 以下にする場合、

$$\sum (i=1 \sim L+1) m C i$$

となる。ここで $m C i$ は m 個のなかから i 個を選ぶ組合せの数である。従って例えば L を15とした場合、その候補数は約1030程度となり、実用上安全であると言える。しかしながら、この方法の場合、繰り返し処理におけるICカードと補助装置の間の通信量が多く、ICカードにおける計算量も大きい。1ブロック512ビットの暗号化に要する、ICカードと補助装置の間の通信量は $m+1$ ブロックである。また、ICカードにおける計算は最大 m 回の法 n 上の乗算が必要である。なお、 m はICカードの秘密データ d の安全性を決定しているパラメータである安全性の面より15程度にする必要がある。このため、1ブロックの暗号化速度はICカード単独で実現する場合に比べてせいぜい一桁高速になるだけである。

そこで、ICカードと補助装置の間の通信量を減少して1ブロックの暗号化時間を短縮する方法も同文献において提案されている。

第3図に従来のべき乗剰余演算装置における第2の例の構成図を示す。120はICカード、121は補助装置である。122、123はそれぞれICカードにおける秘密のデータ p 、 q を格納している p 格納部と q 格納部、124は p と q の積を計算して n を生成する n 生成部、125は n を公開する n 公開部である。126は p 、 q より次の(6)、(7)式を満たす w_p 、 w_q を生成して格納する w_p 、 w_q 生成部である。

$$w_p = q \times (q^{(-1)} \bmod p) \bmod n \quad \dots\dots(6)$$

$$w_q = p \times (p^{(-1)} \bmod q) \bmod n \quad \dots\dots(7)$$

127はある秘密の数 R を格納する R 格納部、128は前記 p 、 q 、 R を用いて次の(8)、(9)を満たす r_p 、 r_q を生成して格納する r_p 、 r_q 生成部である。

信部である。139は前記 y' 送信部より送られてきた y' を受信するICカード内の y' 受信部である。140は前記 y' 、 w_p 、 w_q 、 r_p 、 r_q より次の(12)式を満たす n 以下の数 y を生成する y 生成部である。

$$y = \{ ((y' \bmod p)^{r_p \bmod p}) \times w_p + ((y' \bmod q)^{r_q \bmod q}) \times w_q \} \bmod n \quad \dots\dots(12)$$

141は前記 y を格納する y 格納部である。

なお、前記122～133、139～141はICカード120に含まれ、134～138は補助装置に含まれる。また、122～131、134～135は初期化のときのみに動作する。

次に、以上説明した従来のべき乗剰余演算装置の動作をRSA暗号の復号化を行う場合を例に説明する。なお、RSA暗号の復号化演算は前述した通りである。

<初期化>

① ICカード内の p 、 q (ICカードの秘密の情報)がそれぞれ p 格納部122、 q 格納部

$$r_p = R^{(-1)} \bmod (p-1) \quad \dots\dots(8)$$

$$r_q = R^{(-1)} \bmod (q-1) \quad \dots\dots(9)$$

129はICカードにおける秘密のデータ d を格納している d 格納部、130は前記 d 、 R を入力として次の(10)式を満たす d' を生成する d' 生成部である。

$$d' = d \times R \bmod \lambda(n) \quad \dots\dots(10)$$

131は前記 d' を補助装置に送信する d' 送信部である。132はデータ x を格納している x 格納部、133は x を補助装置に送信する x 送信部である。134は補助装置内で公開値 n を受信する n 受信部、135、136はそれぞれICカードより送られてきた前記 d' 、 x を受信する d' 受信部、 x 受信部である。137は前記134～136の各データを用いて次の(11)式の計算を行い y' を求めるべき乗剰余計算部である。

$$y' = x^{d'} \bmod n \quad \dots\dots(11)$$

138は前記 y' をICカードに送信する y' 送信

部123に格納されている。 n 生成部124において p と q の積を計算して n 公開部125に格納する。 n はこの n 公開部125より広く公開される。 w_p 、 w_q 生成部126においては前記 p 、 q を用いて前記(6)、(7)を満たす w_p 、 w_q を生成して格納しておく。

② ICカード内である秘密の数 R を決め R 格納部127に格納する。 r_p 、 r_q 生成部128ではこの R と前記 p 、 q を用いて前記(8)、(9)を満たす r_p 、 r_q を生成して格納しておく。

③ ICカード内の d (ICカードの秘密の情報)が d 格納部129に格納されている。 d' 生成部130において前記 d と R を用いて前記(10)式を満たす d' を求める。 d' はICカード内の d' 送信部を通して補助装置内の d' 受信部135に格納される。

④ 補助装置内の n 受信部134は公開されている n を受信する。

⑤ 補助装置内の d' 受信部135はICカードより送信された d' を受信する。

＜繰り返し処理＞

以下の処理は612ビットを1ブロックとする
暗号文の数だけ繰り返す。

- ① 暗号文1ブロックをICカード内のx格納部に格納する。
- ② ICカード内のx送信部133より補助装置内のx受信部136に暗号文を送信する。
- ③ 補助装置のべき乗剰余計算部137は暗号文x、公開値n、ICカードから受け取ったd'を用いて前記(11)の計算を行いy'を得る。
- ④ 補助装置内y'送信部は前記べき乗剰余計算部137の出力をICカード内のy'受信部139に送信する。
- ⑤ ICカード内のy生成部140は補助装置が求めたy'とICカード内のwp、wq生成部126、rp、rq生成部128の格納値を用いて前記(12)の計算を行う。なお、上記の方法で求めたyは前記(4)を満たすn未満の正整数である。それは次のI)～III)より証明される。

I) (10)式より次の等式が成り立つ。

II) 上記p上の演算結果と上記q上の演算結果とを中国人の剰余定理を用いて結合して(13)式をもとめる。

- ① p、qに対して次の(16)式を満たすs、tが存在する。

$$p \times s + q \times t = 1 \quad \dots\dots\dots(16)$$

- ② (16)式のs、tは次のように表すことができる。

$$s = p^{-1} \mod q$$

$$t = q^{-1} \mod p$$

従って(6)、(7)式より

$$q \times t = wp$$

$$p \times s = wq$$

が成り立つ。

- ③ Aを任意の算術演算結果とするとき次の(17)式が成り立つ。

$$\begin{aligned} (A \mod n) &= (A \mod p) \times wp \\ &+ (A \mod q) \times wq \mod n \end{aligned} \quad \dots\dots\dots(17)$$

今の場合、 $A = (x \cdot d') \cdot (R^{-1})$ であ

$$\begin{aligned} y &= x \cdot d \mod n \\ &= x \cdot (d' / R) \mod n \\ &= (x \cdot d') \cdot (R^{-1}) \mod n \end{aligned} \quad \dots\dots\dots(13)$$

II) n上の演算である(13)式をnの素因数であるp、q上の演算に分けて計算を行う。

(p上の演算)

$$x \cdot d' \mod p = y' \mod p \quad ((11)式より)$$

$$R^{-1} \mod (p-1) = rp$$

((9)式より)

$$\text{従って } (x \cdot d') \cdot (R^{-1}) \mod p$$

$$= (y' \mod p) \cdot rp \mod p$$

.....(14)

(q上の演算)

$$x \cdot d' \mod q = y' \mod q \quad ((11)式より)$$

$$R^{-1} \mod (q-1) = rq$$

((9)式より)

$$\text{従って } (x \cdot d') \cdot (R^{-1}) \mod q$$

$$= (y' \mod q) \cdot rq \mod q$$

.....(15)

る。これに(13)、(14)、(15)をそれぞれ代入すると以下の通りになる。

$$\begin{aligned} y &= \{ ((y' \mod p) \cdot rp \mod p) \\ &\times wp + ((y' \mod q) \cdot rq \mod q) \times wq \} \mod n \end{aligned}$$

従って(4)式を満たす最終結果は(12)式の結果によって得られることが証明された。

なお、(17)式は以下のI) II)によって証明される。

- I) (16)式より、 $wp = 1 \mod p$ 、 $wq = 0 \mod p$ が成り立つ。

従って(17)式の右辺をpで除した剰余は(A mod p)となる。

- II) (16)式より、 $wp = 0 \mod p$ 、 $wq = 1 \mod p$ が成り立つ。

従って(17)式の右辺をqで除した剰余は(A mod q)となる。

また、補助装置に与えられたデータx、d'、nのうちnは公開値であり、xは暗号文であるためこれらよりICカードの秘密データを得ることは出来ない。さらに、補助装置がd'からdを求める

ためには n の素因数分解をすることが必要となるため、 d の解読は 512 ビットの長語長の数の素因数分解と同等に困難であるといえる。

発明が解決しようとする課題

第 2 の従来例の場合、繰り返し処理における IC カードと補助装置との間の通信量はわずか 2 ブロックである。しかしながら、IC カードが行う(12)式の演算には p 、 q のビット数をそれぞれ 256 ビットとすると、512 ビットの暗号化に次の演算が必要である。

・ 256 ビット幅の乗算剰余 (256 ビットの法上の二項乗算) を $x(xp) + x(xq) - 1$ とする。

ただし $x(xp) = (xp$ を 2 進表現したときのビット数) $+ (xp$ を 2 進表現したときの 1 の個数) $- 1$ とする。

なお、実用的にはこの剰余剰余の回数を小さくするように秘密の数 R を選んで処

理の高速化を図る。

・ 512 ビット幅の乗算剰余 (512 ビットの法上の二項乗算) を 2 回

・ 512 ビット幅の加算剰余 (512 ビットの法上の二項加算) を 1 回

これらの演算を例えばマイクロコンピュータ Z-80 (6 MHz) を用いて行うとその処理時間 4.4 秒となる。(ただし、256 ビット幅の乗算剰余の回数を 8 回とする) また、IC カードと補助装置との間の通信を 9600 bps で実現すると仮定した場合その通信時間は 0.11 秒である。これらを足し合わせると 512 ビットの暗号化に補助装置の演算時間をゼロと考えても 4.5 秒かかることになる。本発明はかかる点に鑑み、IC カード側の演算を高速化し、その結果としてトータルの暗号化時間を従来より短縮できるべき乗剰余演算装置を提供することを目的とする。

課題を解決するための手段

本発明は、素数 p と素数 q の積 n を法とし、正整数 d をべき数として入力 x のべき乗剰余演算を

行う装置であり、前記正整数 d と素数 p と素数 q の値を保持し、かつその値が外部から決定あるいは推測できないように構成された第 1 の計算装置と、第 1 の計算装置から送出された第 1 のデータに対して所定の計算を行いその結果を第 2 のデータとして前記第 1 の計算装置に送出する第 2 の計算装置からなり、前記第 1 の計算装置は前記素数 p と q の積 n と、前記正整数 d を $p-1$ で除した剰余 d_1 と、前記正整数 d を $q-1$ で除した剰余 d_2 を計算してこれらの結果を前記第 1 のデータとして前記第 2 の計算装置に送出し、さらに前記第 2 の計算装置から送出された前記第 2 のデータを前記素数 p と q を用いて結合し、法を前記の数 n とし、前記正整数 d をべき数とする入力 x のべき乗剰余値を求めるものであり、前記第 2 の計算装置は前記第 1 の計算装置から送出された前記第 1 のデータから、前記整数 n を法とし前記 d_1 をべき数とする前記正整数 x のべき乗剰余数 y_1 と、前記整数 n を法とし前記 d_2 をべき数とする前記正整数 x のべき乗剰余数 y_2 を計算し、この結果を

前記第 2 のデータとして前記第 1 の計算装置に対して送出することを特徴とするべき乗剰余演算装置である。

作用

本発明は前記した構成により、第 1 の計算装置は最終的に求めたい法 n 上のべき乗剰余演算を法 p と法 q 上の演算に分割して、それぞれを第 2 の計算装置に計算してもらう。第 2 の計算装置は n の素因数 p 、 q を知らないで第 1 の計算装置から与えられたデータより第 1 の計算装置の IC カードの秘密の情報を得ることは困難である。第 1 の計算装置は第 2 の計算装置に計算してもらった 2 つのデータを中国剰余定理を用いて結合して所望の結果を得る。

実施例

第 1 図は本発明の一実施例におけるべき乗剰余演算装置の構成図を示すものである。

第 1 図において、1 は IC カード、2 は補助装置である。3、4 はそれぞれ IC カードにおける秘密のデータ p 、 q を格納している p 格納部、 q

格納部、6は p と q の積を計算して n を生成する n 生成部、8は n を公開する n 公開部である。7はICカードにおける秘密のデータ d を格納している d 格納部、8は秘密のデータ p 、 q 、 d を用いて次の(18)、(19)式を計算して d_1 、 d_2 を求める d 分割部である。

$$d_1 = d \bmod (p-1) \quad \dots\dots\dots(18)$$

$$d_2 = d \bmod (q-1) \quad \dots\dots\dots(19)$$

9、10は前記 d_1 、 d_2 をそれぞれ補助装置に送信する d_1 送信部、 d_2 送信部である。11はデータ x を格納している x 格納部、12は x を補助装置に送信する x 送信部である。13は補助装置内で公開数 n を受信する n 受信部、14、15、16はそれぞれICカードから送信された前記 d_1 、 d_2 、 x を受信する d_1 受信部、 d_2 受信部、 x 受信部である。17は13～16に格納されているデータを用いて次の(20)、(21)式を計算して y_1 、 y_2 を求めるべき乗剰余計算部である。

$$y_1 = x^{d_1} \bmod n \quad \dots\dots\dots(20)$$

$$y_2 = x^{d_2} \bmod n \quad \dots\dots\dots(21)$$

18、19は前記 y_1 、 y_2 をICカードに送信する y_1 送信部、 y_2 送信部である。20、21はICカード内で前記 y_1 、 y_2 を補助装置側から受け取る y_1 受信部、 y_2 受信部である。22は前記 y_1 、 y_2 、 p 、 q を用いて次の(22)、(23)、(24)式を計算して y を生成する y 生成部である。

$$u_1 = y_1 \bmod p \quad \dots\dots\dots(22)$$

$$u_2 = y_2 \bmod q \quad \dots\dots\dots(23)$$

$$y = ((u_2 + q - u_1) \times w \bmod q) \times p + u_1 \quad \dots\dots\dots(24)$$

ただしここで $w = p^{-1} \bmod q$ である。

23は前記 y を格納する y 格納部である。

なお、前記2～12、20～23はICカード1に含まれ、13～19は補助装置に含まれる。また、2～10、13～16は初期化のときのみ動作する。

次に、以上説明した本実施例のべき乗剰余演算装置の動作を、従来例と同様にRSA暗号の復号化を行う場合を例に説明する。

<初期化>

- ① ICカード内の p 、 q (ICカードの秘密の情報)がそれぞれ p 格納部3、 q 格納部4に格納されている。 n 生成部6において p 、 q の積を計算して n 公開部8に格納する。 n はこの n 格納部により広く公開される。
- ② ICカード内の d (ICカードの秘密の情報)が d 格納部7に格納されている。 d 分割部8において d を前記(18)式を満たす d_1 、 d_2 を求める。そして d の代わりに d_1 、 d_2 を送信部9、10を通して補助装置に送信する。
- ③ ICカード内の秘密の情報 p 、 q を用いて $w = p^{-1} \bmod q$ を計算しておく。
- ④ 補助装置内の n 受信部13は公開されている n を受信する。
- ⑤ 補助装置内の d_1 、 d_2 受信部はICカードより送信された d_1 、 d_2 を受信する。

<繰り返し処理>

以下の処理は612ビットを1ブロックとする暗号分の数だけ繰り返す。

- ① 暗号文1ブロックをICカード内の x 格納部に格納する。
- ② ICカード内の x 送信部12より補助装置内の x 受信部16に暗号文 x を送信する。
- ③ 補助装置のべき乗剰余計算部17は暗号文 x 、公開値 n 、ICカードから受け取った d_1 、 d_2 を用いて前記(20)、(21)の演算を行い y_1 、 y_2 を求める。
- ④ 補助装置内の y_1 、 y_2 送信部は前記べき乗剰余計算部17の出力をICカード内の y_1 、 y_2 受信部に送信する。
- ⑤ ICカード内の y 生成部22は補助装置が求めた y_1 、 y_2 をICカードの秘密のデータ p 、 q を用いて前記(22)、(23)、(24)式を計算する。なお、上記の方法で求めた y は
$$y = x^d \bmod n \quad \dots\dots\dots(25)$$
を満たす n 未満の正整数である。それは次の1) により証明される。
- 1) n 上の演算である(25)式を n の素因数 p 、 q 上の演算に分けて計算を行う。

(p 上の演算)

$$\begin{aligned}
 x^d \bmod p &= x^{(d \bmod (p-1))} \bmod p \\
 &= x^{d_1} \bmod p \quad ((18) \text{式より}) \\
 &= y_1 \bmod p \quad ((20) \text{式より}) \\
 &= u_1 \quad ((22) \text{式より}) \\
 &\dots\dots\dots (26)
 \end{aligned}$$

(q 上の演算)

$$\begin{aligned}
 x^d \bmod q &= x^{(d \bmod (q-1))} \bmod q \\
 &= x^{d_2} \bmod q \quad ((19) \text{式より}) \\
 &= y_2 \bmod q \quad ((21) \text{式より}) \\
 &= u_2 \quad ((23) \text{式より}) \\
 &\dots\dots\dots (27)
 \end{aligned}$$

II) 上記求めた p 上の演算結果と q 上の演算結果を中国剰余定理を用いて結合する。

① p, q より次の (28) を満たす W を求める。

$$W = p^{-1} \bmod q \quad \dots\dots\dots (28)$$

② A を任意の算術演算結果とする時、次の (29) 式が成り立つ。

$$\begin{aligned}
 A \bmod n &= \{ (A \bmod q) + q - (A \bmod p) \} \times W \bmod q \times p + (A \bmod p) \\
 &\dots\dots\dots (29)
 \end{aligned}$$

今の場合、 $A = x^d$ である。

これに (26) ~ (27) を代入すると (24) 式が成り立つことが証明される。

なお、(29) 式を計算することによって (26) 式を満たす y が求められることは次の (I) ~ (III) により証明される。

(I) (29) 式の右辺は n 未満の値である。

〔理由〕

$$\begin{aligned}
 &\{ (A \bmod q) + q - (A \bmod p) \} \times W \bmod q \leq q - 1 (A \bmod p) \leq \\
 &p - 1 \text{ であることより}
 \end{aligned}$$

$$\begin{aligned}
 &\text{従って (29) 式の右辺} \leq (q - 1) \times p + (p - 1) \\
 &= p \times q - 1 < n
 \end{aligned}$$

(II) (29) 式右辺の法 p における値が $(A \bmod p)$ となることは自明である。(III) (29) 式右辺の法 q における値が $(A \bmod q)$ となる。

〔理由〕

(28) 式の W を (29) 式に代入して法 q における値を求めると

$$\begin{aligned}
 &\{ (A \bmod q) + q - (A \bmod p) \} \\
 &\times p^{-1} \bmod q \times p + (A \bmod p) \bmod q \\
 &= (A \bmod q)
 \end{aligned}$$

となる。

また、 d_1, d_2 より d を求めるためには n の素因数分解をすることが必要となるため、素因数 p, q を知らない補助装置にとって d の解読は 512 ビットの長語長の数の素因数分解と同等に困難であると言える。この点では従来の第 2 の実施例と同じ安全性であると言える。

繰り返し処理時における IC カードと補助装置との間の通信量は IC カードから補助装置に 1 ブロック、補助装置から IC カードに 2 ブロックの

計 3 ブロックである。この通信量は 9600 bps で通信を行うと仮定したとき 0.16 秒に相当する。また、IC カードが行う (22) ~ (24) の演算には次の演算が必要である。

- ・ 256 ビット幅の剰余演算を 2 回
- ・ 256 ビットの乗算剰余演算を 1 回
- ・ 256 ビットの乗算を 1 回
- ・ 256 ビットの加算を 2 回
- ・ 512 ビットの加算を 1 回

これらの演算を例えばマイクロコンピュータ Z-80 (6 MHz) を用いておこなうとその処理時間は約 0.975 秒となる。ただし、256 ビットの剰余演算の処理時間を 0.175 sec / 1 回、256 ビットの乗算時間を 0.175 sec / 1 回、256 ビットの乗算剰余の演算時間を 0.36 sec / 1 回、256 ビットの加算時間を 0.025 sec / 1 回、512 ビットの加算時間を 0.05 秒 / 1 回としている。従って、通信時間と IC カードにおける処理時間を足し合わせると 1.135 秒になる。従来例と同様に補助装置の演算時間をゼロと

考えると1.136秒で512ビットの暗号化が実行されることになる。

以上のように、本実施例によれば通信量は従来よりも多少増加するが、ICカード側の演算を軽減することによってトータルとして従来例の約4倍の速度アップを得ることができる。

なお、この実施例においては(24)式に示した効率的な中国人の剰余定理を用いたが、従来例と同様(12)式に示した式で法 p 上の演算結果と法 q 上の演算結果を結合しても良い。

発明の効果

以上説明したように、本発明によれば繰り返し処理において第1の計算装置は最終的に求めたいべき乗剰余演算の「べき乗」の部分を実行してもらい、そのため、第1の計算装置におき、中国人の剰余定理を用いて第2の計算装置の行った演算結果を結合する際、その演算の中にはべき乗剰余演算が含まれていない。これによって、第1の計算装置の負担する演算が従来(第2の従来例)に比べて4倍以上軽減する。

第2の計算装置の行う演算量はべき乗のビット数を考えると従来と同等であることが分かる。

また、第1の計算装置と第2の計算装置の間の通信量は従来例の1.5倍になるが、通信速度を例えば9600bpsと考えると従来例との通信時間の差は非常に小さい。

以上のことより、処理時間のトータルとしては1回の繰り返しについて従来例の4倍の高速化が達成できている。

第1の計算装置の保持している秘密データの安全性については、第2の計算装置が得ている d_1 、 d_2 から d を得る困難さが n の素因数分解を行う困難さと同等であると考えられるため、 n を512ビット程度にすることによって保証される。この点は従来と同じである。

これらのことより本発明の実用的効果は大きい。

4. 図面の簡単な説明

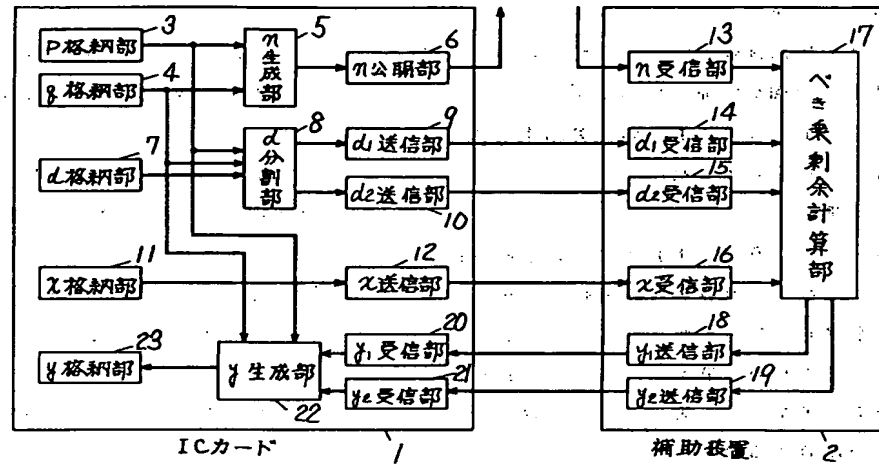
第1図は本発明における一実施例のべき乗剰余演算装置のブロック図、第2図は第1の従来例のべき乗剰余演算装置のブロック図、第3図は第2

の従来例のブロック図である。

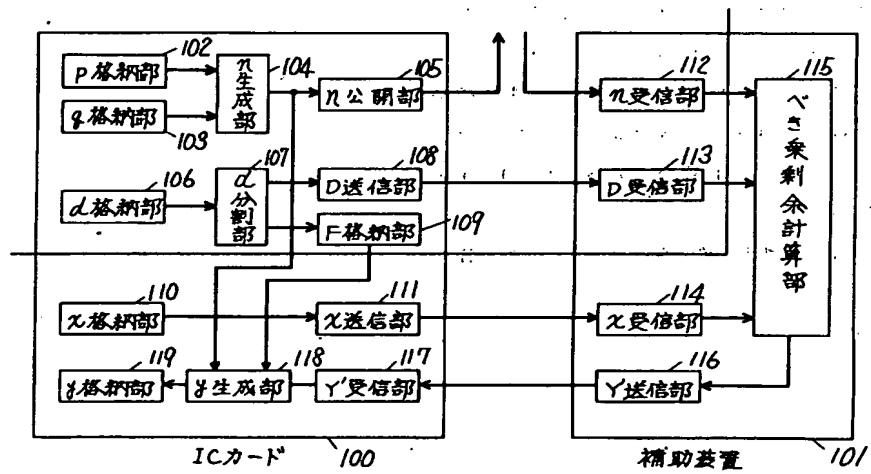
1, 100, 120……ICカード、2, 101, 121……補助装置、3, 102, 122…… p 格納部、4, 103, 123…… q 格納部、5, 104, 124…… n 生成部、6, 105, 125…… n 公開部、7, 106, 129…… d 格納部、11, 110, 132…… x 格納部、17, 115, 137……べき乗剰余計算部、23, 119, 141…… y 格納部。

代理人の氏名 弁理士 栗野重孝 ほか1名

第 1 図



第 2 図



第 3 図

